PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GB030011	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/EP2004/050847	International filing date *(day/month/year)* 25.05.2004	Priority date *(day/month/year)* 04.06.2003
International Patent Classification (IPC) or national classification and IPC G06F1/00, H04L9/08		
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☐ *sent to the applicant and to the International Bureau)* a total of sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
24.03.2005	02.08.2005
Name and mailing address of the international preliminary examining authority: European Patent Office - Gitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840	Authorized Officer Carnerero Álvaro, F Telephone No. +49 30 25901-

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/050847

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:

   - ☐ international search (under Rules 12.3 and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4)
   - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

   Description, Pages

   1-12 as originally filed

   Claims, Numbers

   1-24 as originally filed

   Drawings, Sheets

   1-6 as originally filed

   ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:

   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/EP2004/050847

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-24
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

1. The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: CHOUDHURY A K ET AL: "COPYRIGHT PROTECTION FOR ELECTRONIC PUBLISHING OVER COMPUTER NETWORKS" IEEE NETWORK, IEEE INC. NEW YORK, US, vol. 9, no. 3, 1 May 1995 (1995-05-01), pages 12-20, XP000505280 ISSN: 0890-8044

D2: MENEZES, OORSCHOT, VANSTONE: "Handbook of applied cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 548, 549, 552, 577-581, XP002302982 BOCA RATON, FL, US ISBN: 0-8493-8523-7

2. The present application does not meet the requirements of Article 33(3) PCT, because the subject-matter of the claims does not involve an inventive step.

2.1 Document D1 discloses (see page 15, left-hand column, paragraph 5 to right-hand column, paragraph 4; page 16, right-hand column, paragraph 5, to page 17, left-hand column, paragraph 7; figure 2) a method for the encrypted delivery of information by a publisher to one or more recipients, wherein a trusted body (referred to as "copyright server") distributes the keying material needed for decrypting the information to the different recipients. D1 also mentions the use of asymmetrical encryption techniques.

2.2 Document D2, for its part, discloses (pages 577 to 581) the concept of key life-cycle management. See in particular, on pages 578 to 580, the distinction between the notions of user registration and initialization and key generation, on one hand, and key installation and "normal use" on the other. Similarly, see on page 580 and figure 13.10 the distinction between the pre-operational and the operational states of cryptographic keys during their life cycle: only after the installation of keying material takes place, at specific times determined by the management scheme being implemented, does said keying material become operational.

By virtue of the very definition of the concept of cryptographic keys, the management of the times at which decryption keys are made available for operational use allows to

regulate the accessibility of the encrypted information associated with said keys.

Document D2 also discloses (pages 548, 549, 552) the principle of asymmetrical key pair generation by a trusted third party and the separate delivery by said party of the private and public components of the pair (in the latter case, by dint of a digital certificate) to the receiver and the sender of a given encrypted message respectively. In addition, page 549, paragraph 13.4 (iii)-2 states that the trusted party can take charge of managing the life-cycle of the keys (thereby enforcing the times at which they are distributed and rendered operational).

2.3 It would be a matter of normal design procedure for the person of skill in the art to use the above teachings from D2, which is a widely-used reference book (PCT International Search and Preliminary Examination Guidelines PCT/GL/ISPE/1 13.13) and deals with issues of direct relevance to the subject-matter of D1 (i.e. key management; PCT International Search and Preliminary Examination Guidelines PCT/GL/ISPE/1 13.14, in particular 13.14(a)), to improve the cryptographic schemes which underlie the electronic publishing methods disclosed in document D1.

In so doing, one would arrive at a method for the control of the disclosure times of decryption keys and the information associated therewith corresponding to that of independent claim 1, which therefore is not deemed to involve an inventive step (Article 33(3) PCT).

2.4 The same reasoning applies to independent claims 9, 20, 23 and 24.

2.5 The dependent claims do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step, since their contents are covered by D1 or D2 or belong to the general technical knowledge in the field of cryptography.

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (SEPARATE SHEET)

International application No.

PCT/EP2004/050847